Amendments to the Specification

Please replace paragraph [0003] with the following paragraph:

[0003] This Public Key Infrastructure (PKI) enables users of an unsecured public network, such as the Internet, to securely and privately exchange data, communication and/or currency over the network. An essential component of PKI is a digital certificate (certificate). The certificate is basically a bit of information that says that a particular computer or web server is trusted by an independent source known as a certificate authority. The certificate authority acts as an intermediary between both computers, and can confirm that each computer is in fact who it claims to be, and notarizes the public keys of each computer to the other. By signing the public key, the certificate authority asserts the identity of the subject/computer, the public key, and characteristics belonging to the subject/computer. The public key mathematically binds the certificate to its bearer, or to be exact, to the bearer's private or secret key. With certificates, it is possible to check the chain of trust that relates to the certificate and the public key, and through the certificate status checking ~~mechanismto~~ mechanism to make sure the secret known only by the certificate bearer (i.e., private key) has not leaked.